

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

COMMODITY FUTURES TRADING
COMMISSION,

Plaintiff,

v.

JOHN PATRICK GORMAN III,

Defendant.

Case No. 21-cv-870 (JGLC)

ECF Case

[PROPOSED] STIPULATED PROTECTIVE ORDER

WHEREAS, Plaintiff Commodity Futures Trading Commission (“CFTC”) and Defendant John Patrick Gorman III (“Defendant”) (hereinafter referred to collectively as “Parties” or any one individually as a “Party”), through their respective counsel of record, anticipate that discovery in this action (the “Action”) is likely to involve the disclosure of confidential or sensitive commercial, personal, financial and/or business information; and

WHEREAS, the Parties desire to enter into an agreement pursuant to Rule 26(c) of the Federal Rules of Civil Procedure to protect such confidential or sensitive commercial, personal, financial and/or business information (“Protective Order”);

It is hereby STIPULATED, AGREED, and ORDERED as follows:

A. **Scope**

1. This Protective Order shall govern the use of all materials or other information supplied or produced in the course of discovery, including initial disclosures, responses to discovery requests, and deposition testimony and exhibits, by and among the Parties and any non-parties to the Action in connection with discovery in the Action, whether supplied or produced pursuant to a formal discovery request or subpoena, a request made at a deposition, or any other

formal or informal means (such information hereinafter referred to as “Discovery Material”). This Protective Order shall also govern the redacted filing of certain information and applications for filing certain information under seal in connection with this Action. All Parties to this Action and their attorneys, as well as non-party participants, shall comply with the terms and procedures set forth below with respect to documents and materials produced and/or disclosed in discovery. Notwithstanding anything else contained herein, nothing in this Protective Order shall in any way limit the right of a producing or supplying party (hereinafter “Producing Party”) to make whatever use it deems appropriate of its own documents.

2. All Discovery Material produced in the Action shall be used only for the purposes of prosecuting, defending, or appealing the Action and shall not be disclosed to any person, except for uses and disclosures made in accordance with the terms hereof, including but not limited to those described in Section A, or as otherwise required or authorized by law. The attorneys of record for the Parties and all other persons receiving Discovery Material governed by the Protective Order shall take all reasonable steps to ensure that the Discovery Material governed by the Protective Order is: (i) used only for the purposes specified herein; and (ii) disclosed only to authorized persons. In particular, Discovery Material may not be used for any commercial, business, or other purpose. However, nothing in this Protective Order shall be construed to limit a Producing Party’s use of its own confidential Discovery Material in any manner.

3. Under this Protective Order, any Producing Party shall have the right to identify and designate Discovery Material as “Confidential” when the Producing Party in good faith believes it contains proprietary, confidential, commercially sensitive information, personally identifiable information protected under the Privacy Act of 1974, 5 U.S.C. § 552a, material protected under Sections 8(a) and 23(h)(2) of the Commodity Exchange Act, 7 U.S.C. §§ 12(a),

26(h)(2), or other confidential research, development, or commercial information as such terms are used in Fed. R. Civ. P. 26(c)(1)(G) whether embodied in documents, physical objects, or factual knowledge of persons.

4. Any Producing Party shall have the right to identify and designate Discovery Material as “Highly Confidential” when the Producing Party in good faith believes it contains extremely sensitive information including, but not limited to, material protected under Sections 8(a) and 23(h)(2) of the Commodity Exchange Act, 7 U.S.C. §§ 12(a), 26(h)(2), such as transaction data, non-public proprietary information, the identities of whistleblowers, and market positions, whether embodied in documents, physical objects or factual knowledge of persons.

5. This Protective Order does not govern the assertion or applicability of privileges, except for the limitations on waiver discussed in Paragraphs E.5 or G.2.

6. After the Court enters the Protective Order, a copy of this Protective Order shall be served along with any subpoena served in connection with this Action. A non-party who is obligated to provide discovery in this Action by deposition, production of documents, or otherwise, shall be afforded the protections of this Protective Order upon signing the declaration attached hereto as Exhibit A. By signing such declaration, the non-party also agrees to be bound by the terms of the Protective Order.

7. This Protective Order constitutes a court order within the meaning of the Privacy Act of 1974, 5 U.S.C. § 552a(b)(11) and implementing regulations, providing a basis for release of the requested documents and records to Defendant without obtaining prior written consent of the individuals to whom the records pertain, pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a(b)(11) and Rule 26(c) of the Federal Rules of Civil Procedure. Any such record produced in this Action must be strictly protected in accordance with this Protective Order.

B. Designation of Confidentiality

Discovery Material may be designated Confidential or Highly Confidential within the meaning of this Protective Order as follows:

1. A Producing Party shall, if appropriate, designate Discovery Material as “Confidential” or “Highly Confidential” by stamping or labeling each page of the Discovery Material, in a manner which will not interfere with its legibility, the words “CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER” (or “CONFIDENTIAL” if space is limited), or “HIGHLY CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER” (or “HIGHLY CONFIDENTIAL” if space is limited), and may also include a field in the metadata in the production of such Discovery Material. Unless it would obscure, conceal, or interfere with any information originally appearing in the underlying image, any confidentiality designation pursuant to the Protective Order shall appear on the lower left-hand side of each image. To protect the confidentiality of files produced in Native Format,¹ any confidentiality designations pursuant to the Protective Order shall appear on the associated slip-sheet.

2. For Discovery Material that cannot be designated in the manner described in Paragraph B(1) above, the Producing Party may designate such Discovery Material as Confidential or Highly Confidential by stamping or labeling the Discovery Material itself or the exterior of the container(s)/media in or on which the Discovery Material is stored with the label that appears in Paragraph B(1), above.

3. The designation of Discovery Material as Confidential or Highly Confidential shall be made prior to, or contemporaneously with, the production or disclosure of that Discovery

¹ “Native Format” means the file format of ESI in the application in which such ESI was originally created.

Material, except that inadvertent or unintentional disclosure of Discovery Materials shall be governed in accordance with Paragraph G.

4. Portions of depositions shall be deemed Confidential or Highly Confidential only if they are designated as such when the deposition is taken or are so designated within thirty (30) days after receipt of the transcript(s) by counsel for a Party or the deponent. All information disclosed in a deposition shall be treated as Confidential until thirty (30) days after the transcript(s) of said deposition is actually received by counsel for such party or the deponent to provide the opportunity for making the Confidential or Highly Confidential designation provided herein.

C. Disclosure of Confidential Information

1. Absent consent of the Producing Party, Discovery Material designated Confidential pursuant to this Protective Order and copies, duplicates, or extracts of such Discovery Material, or summaries or descriptions that disclose Confidential information from such Discovery Material, shall only be disclosed or made available by counsel for the Party receiving such Discovery Material to the following persons:

- a. Counsel of record for the Parties, employees and agents of counsel, and CFTC employees and agents;
- b. the Defendant;
- c. outside consultants, investigators, or experts (collectively, "experts") retained by the Parties to assist in the preparation and trial of this Action to whom it is necessary that Discovery Material designated as Confidential under this Protective Order be shown in connection with the preparation and trial of this Action; provided, however, that prior to any such person receiving any Discovery Material designated as Confidential, the person shall execute a copy of EXHIBIT A ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE;
- d. any person identified in such materials as the author, sender, addressee, or copy recipient of the Confidential information, or who was a Custodian² of the Confidential information, provided that prior to such disclosure to any of the

² "Custodian" means the Person who is in possession, custody, or control of responsive ESI.

foregoing other than the Producing Party, the disclosing party shall use reasonable best efforts to cause the person to whom the Confidential information is to be disclosed to execute a copy of EXHIBIT A - ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE;

- e. any potential witness in this Action to whom it is necessary for purposes of the litigation that the Discovery Material designated as Confidential under the Protective Order be shown; provided, however, that prior to the disclosure any potential witness shall be provided with a copy of this Protective Order and the Parties shall use their reasonable best efforts to cause the potential witness to execute a copy of EXHIBIT A - ACKNOWLEDGEMENT AND DECLARATION OF COMPLIANCE;
- f. any witness being examined in this Action in deposition or at trial to whom it is necessary that the Discovery Material designated as Confidential under this Protective Order be shown in connection with the examination, and their counsel; provided, however, that prior to such disclosure any such witness shall be provided with a copy of this Protective Order and the Parties shall use their reasonable best efforts to cause such witness to execute a copy of EXHIBIT A - ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE;
- g. the Court and its personnel, as well as court reporters and recorders engaged for depositions;
- h. any other person or entity authorized by law; and
- i. any other person only upon order of the Court or upon stipulation of the Producing Party.

D. Disclosure of Highly Confidential Information

1. Absent consent of the Producing Party, Discovery Material designated Highly Confidential under this Protective Order and/or any information derived therefrom shall only be disclosed or made available by counsel of the Party receiving such Discovery Material to the following persons:

- a. counsel of record for the Parties;
- b. employees or agents of Parties to whom it is necessary that Discovery Material designated as Highly Confidential under this Protective Order be shown in connection with the preparation and trial of this action; provided, however, that prior to any such person receiving any Discovery Material designated as Highly Confidential, the person shall execute a copy of EXHIBIT A - ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE; also

provided that nothing in this Paragraph will prohibit using Highly Confidential information, in summary form and not including information or data that is or may be identifiable as information of any third party, in evaluations, analyses or reports provided to senior management or other necessary employees in connection with any attempt to settle or otherwise resolve the Action;

- c. experts retained by the Parties to assist in the preparation and trial of this Action; provided, however, that prior to any expert receiving any Discovery Material designated as Highly Confidential, the expert shall execute a copy of EXHIBIT A - ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE;
- d. any person identified in such materials as the author, sender, addressee, or copy recipient of the Highly Confidential information, or who was a Custodian of the Highly Confidential information, provided that prior to such disclosure to any of the foregoing other than the Producing Party, the disclosing party shall use reasonable best efforts to cause the person to whom the Highly Confidential information is to be disclosed to execute a copy of EXHIBIT A - ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE;
- e. any potential witness in this Action to whom it is necessary for purposes of the litigation that the Discovery Material designated as Highly Confidential under the Protective Order be shown; provided, however, that prior to the disclosure any potential witness shall be provided with a copy of this Protective Order and the Parties shall use reasonable best efforts to cause the potential witness to execute a copy of EXHIBIT A - ACKNOWLEDGEMENT AND DECLARATION OF COMPLIANCE;
- f. any witness being examined in this Action in deposition or at trial to whom it is necessary that the Discovery Material designated as Highly Confidential under Protective Order be shown in connection with the examination, and their counsel, provided, however, that prior to such disclosure any such witness shall be provided with a copy of this Protective Order and the Parties shall use their reasonable best efforts to cause such witness to execute a copy of EXHIBIT A - ACKNOWLEDGEMENT AND DECLARATION OF COMPLIANCE;
- g. the Court and its personnel, as well as court reporters and recorders engaged for depositions;
- h. any other person or entity authorized by law; and
- i. any other person only upon order of the Court or upon stipulation of the Producing Party.

E. Restrictions and Procedures Regarding Confidential or Highly Confidential Information

1. Counsel of record are responsible for employing reasonable measures to control access to and distribution of information designated Confidential or Highly Confidential. Except as provided in Paragraphs C(1)(a-i) and D(1)(a-i) above, counsel for the Parties must maintain all Confidential information in a reasonably secure manner so that it is not disclosed or used in a manner inconsistent with this Protective Order. Specifically with regard to Confidential or Highly Confidential information produced by the Commission in this action on electronic storage media, the Receiving Party must maintain, transmit, and store such data using industry standard, off-the-shelf encryption programs and tools.

2. All copies, duplicates, or extracts of such Discovery Material, or descriptions that disclose Confidential information from such Discovery Material (hereinafter referred to collectively as “copies”), designated as Confidential or Highly Confidential under this Protective Order or any portion thereof, shall be immediately affixed with the words “CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER” or “HIGHLY CONFIDENTIAL – SUBJECT TO PROTECTIVE ORDER” if those words do not already appear.

3. If Confidential or Highly Confidential information is to be discussed or disclosed during a deposition, any Party shall have the right to exclude from attendance at the deposition, during the time the Confidential or Highly Confidential information is to be discussed, any person or entity not entitled under this Protective Order to receive such Confidential or Highly Confidential information.

4. To the extent that any materials subject to this Protective Order (or any pleading, motion, memorandum, affidavit or other papers referring to them) are proposed to be filed or are filed with the Court, the filing of those materials and papers, or any portion thereof, which disclose

Confidential or Highly Confidential information, shall conform with Federal Rule of Civil Procedure 5.2 and with the Court's Rules of Individual Practice. The Parties shall be allowed to file or otherwise publish with the Court Confidential information, but not Highly Confidential information, provided any sensitive personal identifying information is redacted, and such information is material to any facts or issues in this proceeding. If a Party determines it must file Highly Confidential information that is material to any facts or issues in this proceeding, the Party shall move to file the information under seal.

5. No Discovery Material containing Highly Confidential information shall be made public at a hearing or at trial absent agreement of the Producing Party permitting such disclosure or an application, which may be oral, to the Court for a ruling. Any Party intending to use at a hearing any Discovery Material designated Confidential or Highly Confidential by another Party shall, where reasonable, give advance written or oral notice to the Producing Party so that the Parties may discuss in advance of or at the hearing proposed procedures for handling such Discovery Material. Nothing contained in this paragraph shall be deemed to prohibit the use or introduction of otherwise Confidential or Highly Confidential documents at trial in the event the Court rules against any application to preserve confidentiality or circumstances that make it impractical for the Parties to provide each other with advanced written notice.

6. In the event any Discovery Material designated as Confidential or Highly Confidential is lost, accessed by or disclosed to any person not authorized by this Protective Order to receive the Discovery Material, the Party responsible for the loss, unauthorized access, or unauthorized disclosure shall immediately after discovery of such situation:

- a. notify any person or entity to whom disclosure was made that the disclosure contains Confidential information subject to this Protective Order;
- b. take appropriate action to cure and prevent any further risk of loss, unauthorized access or disclosure of the information; and

- c. notify the Producing Party of the loss, unauthorized access, or disclosure and reasonably cooperate with the Producing Party to address and remedy the loss, unauthorized access, or disclosure.

The identification under this section of a party to whom disclosure was made shall not constitute a waiver of attorney work product or attorney-client privileges. Nothing contained in this Order shall be deemed or relied upon to limit the rights of the Parties to seek equitable or other relief from the responsible Party in the event of a loss, or unauthorized access or disclosure of Confidential or Highly Confidential information, or create any right or benefit, substantive or procedural, for any person or entity other than the Parties.

8. In the event disclosure of any Discovery Material designated as Confidential or Highly Confidential is sought from anyone subject to this Protective Order pursuant to a lawful subpoena or other legal process, such person or entity shall upon receipt of such request, notify the Producing Party within seven (7) business days and provide a copy of the subpoena or process and the date set for production, if specified. The Producing Party may then seek to prevent disclosure by filing a motion for protective order or to take other appropriate action within a reasonable time, under the circumstances, but in any event prior to the date set for production, and the Confidential or Highly Confidential Discovery Material shall not be disclosed until resolution of any such challenge to the subpoena or process.

9. Notwithstanding any other terms in this Protective Order, the Producing Party may redact or withhold particularly sensitive personally identifiable information that is not relevant, the unauthorized disclosure of which could result in substantial harm to an individual. Any redacted material must be clearly labeled as having been redacted. The Producing Party shall provide the Receiving Party with a log of the documents withheld or redacted for privilege in the form specified by Federal Rule of Civil Procedure 26(b)(5) and Local Civil Rule 26.2, unless otherwise agreed to by the parties or ordered by the Court.

10. Upon execution, the Parties agree to be bound by the terms of this Protective Order pending its entry by the Court, or pending the entry of an alternative thereto which is satisfactory to all Parties, and any violation of its terms shall be subject to the same sanctions and penalties as if this Protective Order had been entered by the Court. The Parties may not disclose any Confidential or Highly Confidential material to any party joined as an additional party to the Action unless and until such additional party has agreed in writing to be bound by the terms of this Protective Order.

11. The Producing Party may withdraw the designation of Confidential or Highly Confidential at any time during the pendency of this matter.

F. Challenging Designation of Confidentiality

1. If any Party disputes whether any Discovery Material is properly designated as Confidential or Highly Confidential, the Parties agree to attempt to resolve such dispute among themselves. The Party who disputes the designation shall provide notice of its objection to the Producing Party. The Producing Party shall then respond in writing within fourteen (14) business days with its reason(s) for its designation. The Parties will then confer, at a time and in a manner mutually agreeable, and make reasonable efforts to resolve their differences. In the event the Parties are not able to resolve the dispute, the designation of confidentiality may be challenged upon motion by the party challenging the designation. The burden of persuasion in any such challenge proceeding is on the Party asserting such confidentiality. However, a Party shall not be obligated to challenge the propriety of a designation at the time made, and failure to do so shall not preclude a subsequent challenge thereto. The party challenging a “CONFIDENTIAL” designation must obtain a court order before disseminating the information to anyone other than the parties specified in Paragraphs C and D.

G. Inadvertent or Unintentional Disclosure

1. If a Party inadvertently produces or provides Discovery Material that contains any Confidential or Highly Confidential information without designating it Confidential or Highly Confidential as provided in this Protective Order, it may be disclosed to others until the Receiving Party is notified of the error by the Producing Party and/or the party whose Confidential or Highly Confidential information was disclosed. The Producing Party may give written notice to the Receiving Party that the Discovery Material is Confidential or Highly Confidential and should be treated in accordance with the provisions of this Protective Order. As soon as the Receiving Party receives such notice, the Confidential or Highly Confidential information must be treated as if it had been timely designated under this Protective Order, and the Receiving Party must make good faith efforts to retrieve copies of the Discovery Material which it distributed or disclosed to persons not authorized to access such Confidential or Highly Confidential information, as well as retrieve copies made by all such persons, and must inform all such persons that the Confidential or Highly Confidential information is so designated and is subject to this Protective Order.

2. If during the review of any unmarked Discovery Material the Receiving Party has actual knowledge that such Discovery Material clearly contains Confidential or Highly Confidential information, the Receiving Party must promptly notify the Producing Party in writing and sequester the Discovery Material until the Producing Party has had a reasonable opportunity to respond. Counsel for the Producing Party is responsible for providing substitute copies of Confidential or Highly Confidential Discovery Material marked in accordance with this Protective Order, and counsel for the Receiving Party must return or confirm in writing the destruction of unmarked copies upon receipt of any such substitute copies.

3. If a Producing Party discovers that it has inadvertently disclosed privileged or protected Discovery Material, it shall promptly notify the Receiving Party of the production in writing, which notice shall identify the inadvertent disclosure(s) and may direct the Receiving Party to promptly return, destroy, or make inaccessible the Discovery Material and all copies thereof. Within five (5) days of receipt of such notice, the Receiving Party shall inform the Producing Party that compliance will be effectuated or otherwise challenge the claim or privilege or other protection in writing. If the claw-back notice is challenged, the Parties will meet and confer within ten (10) days to attempt to resolve the dispute. The Receiving Party shall: (i) neither use nor disclose the Discovery Material (except as is necessary for the purpose of challenging the claim of privilege or legally cognizable protection and otherwise only in the event that the challenge is resolved against the Producing Party's claim of privilege or legally cognizable protection); and (ii) within twenty-one (21) days of receipt of such notice, and in accordance with the Producing Party's reasonable instructions, destroy, return, or disable all access to the Discovery Material (but in the case of a challenge to the claim of privilege or legally cognizable protection, the Receiving Party may retain one copy for the purpose of challenging the privilege or legally cognizable protection claimed or the inadvertency of the disclosure). In all cases, the Receiving Party will endeavor in good faith to retrieve any copies of such Discovery Material, to return, destroy, or otherwise dispose of the materials, and take all steps necessary to prevent disclosure by the Receiving Party of the Discovery Material.

4. If during the review of Discovery Material the Receiving Party has actual knowledge that such Discovery Material contains privileged information, which includes confidential informant and or deliberative process privilege, or information otherwise subject to legally cognizable protection, such Receiving Party shall immediately refrain from examining the affected

Discovery Material and shall promptly notify the applicable Producing Party in writing that the Receiving Party possesses potentially privileged information or potentially protected information, as applicable. The Receiving Party's treatment of such material shall be in accordance with Federal Rule of Civil Procedure 26(b)(5)(B).

5. The Parties further agree not to assert that such inadvertent or mistaken disclosure of such Discovery Material by itself constitutes a waiver by the Producing Party of any claims of privilege or work-product immunity. Further, this order constitutes an order under Federal Rule of Evidence 502(d) that any inadvertent disclosure of attorney-client privileged and/or work-product protected information does not waive that privilege or protection. However, nothing herein restricts the right of the Receiving Party to challenge the Producing Party's claim of privilege if appropriate within a reasonable time after receiving notice of the inadvertent or mistaken disclosure.

H. Procedures and Protocols Governing the Location, Collection, and Production of Hard-Copy Documents and Electronically Stored Information

1. Format Guidelines. The Parties shall, to the extent reasonably and technically possible, produce documents according to the specifications provided in this Protective Order and in Exhibit B.

2. De-NISTing. Electronically Stored Information³ shall be filtered for file type to remove system files, program files, and other non-user created data files that are on the industry standard list of such files maintained by the National Institute of Standards & Technology

³ “Electronically Stored Information” or “ESI” is equal in scope to “electronically stored information” in Fed. R. Civ. P. 34(a)(1)(A) and includes information or data (including files, databases, and programs) stored or recorded in or on electronic, digital, magnetic, or similar Media. ESI includes Electronic Communications.

(“NIST”). The Parties recognize that to reduce the document review population, additional file types may need to be excluded.

3. Deduplication. A Party is required to produce only a single copy of a responsive family group. Each Party may remove exact duplicate family groups (i.e., identical copies of the same document(s)), to reduce the unnecessary cost of reviewing and producing exact duplicate documents. If a Party chooses to remove exact duplicate documents, the Party shall make reasonable efforts to remove exact duplicate ESI according to the MD5 or SHA-1 hashing method and additional information regarding the family relationship⁴ and shall identify in the “All Custodians” field of each document the name(s) of the custodians whose documents the Producing Party agreed to produce who had duplicates of the document removed during processing. Moreover: (1) if a document is a duplicate of another document but the documents have different family members, they will not be de-duplicated,⁵ although each family member shall be hashed separately for purposes of populating the “MD5 or SHA-1 Hash” field in Exhibit B; (2) responsive non-privileged attachments to documents shall not be disassociated from the parent document even if they are exact duplicates of another document in the production; and (3) hard-copy documents shall not be eliminated as duplicates of responsive ESI. ESI that is not an exact duplicate according to the MD5 or SHA-1 hashing method may not be removed. However, a Producing Party may use email threading—that is, to enable the Producing Party to produce the most inclusive subset of emails in a responsive population—to defensibly exclude, from both review and production,

⁴ “Family Relationship” means the association between an attachment and its parent document or between embedded documents or linked internal or non-public documents and their parents.

⁵ Unless otherwise agreed by the Parties, a Family Group can only be removed through de-duplication if each and every member of the de-duplication candidate Family Group has identical MD5 or SHA-1 hash codes to the corresponding members of another Family Group. For example, if there is a two-member Family Group with a parent and an attachment, the MD5 hash codes of the parent must be identical and the MD5 hash codes of the attachments must also be identical.

duplicative content within the Producing Party's documents. Both de-duplication and email threading shall be performed with careful consideration of full family groups, and therefore, neither process will suppress unique content found in an attachment. The Producing Party shall produce separate inclusive emails where a thread splits into different conversation "branches."

4. Encrypted Documents. The Parties will make reasonable efforts to ensure that any responsive documents identified that are encrypted or password-protected are successfully processed for review and production under the requirements of this Stipulation, and if produced in Native Format, the decrypted document is produced. To the extent responsive encrypted or password-protected documents are successfully processed according to the requirements of this Stipulation, the Parties have no duty to identify the prior encrypted status of such documents. To the extent such responsive documents are not successfully processed despite use of reasonable efforts, including reasonable technical efforts to obtain passwords, a placeholder TIFF⁶ image may be produced in place of each such document indicating that security protection could not be removed. Upon request from the Receiving Party, the Parties shall meet and confer in good faith regarding reasonable efforts or mechanisms that could be undertaken to remove such security protection or the production of available Metadata.⁷

⁶ "TIFF" or Tagged Image File Format refers to the CCITT Group IV graphic file format for storing bit-mapped images of ESI or scanned Hard-Copy Documents.

⁷ "Metadata" means (i) structured, i.e., fielded, information embedded in a Native Format file which describes, *inter alia*, the characteristics, origins, usage, and/or validity of the electronic file; and (ii) information generated automatically by the operation of a file system or application when a native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system.

5. Documents to Be Produced in Native Format. As provided in Exhibit B:

- a. Microsoft Excel and other spreadsheet files, including comma or tab delimited text files, photographs, video files, audio files, animation files, and other multi-media files shall be produced in Native Format, if available.
- b. Photographs, PowerPoint, and other presentation files may be produced either in Native Format or as color images in TIFF format.
- c. The Parties agree to meet and confer regarding the ability to produce other file types in Native Format.

6. The production Load Files⁸ shall contain a link to the produced Native Format files as specified in the “NativePath” Metadata field described in Exhibit B. Each electronic file produced in Native Format shall be assigned a unique Bates Number, as set forth in Section H(12) of this Protective Order and Section III of Exhibit B to this Protective Order, and the database record for that file shall include a single page Bates-stamped TIFF image slip-sheet bearing the phrase “PRODUCED IN NATIVE FORMAT” (or similar language). Files produced in Native Format shall be given file names that include the Bates Number and the file extension.

7. Production of Additional Documents in Native Format. Each Party reserves the right to request production in Native Format for any ESI that it believes is not adequately represented in the TIFF format specified in Exhibit B and, upon a showing of reasonable need, such requests will not be unreasonably denied.

⁸ “Load File” means the electronic file that is used to import all required production information into a document database, including, as applicable: document images; Extracted Text or OCR Text; Native Format files where required by this Protective Order; Metadata; information related to the embedded content of a document; and information indicating document breaks and document relationships, such as the relationship between an Electronic Communication and its attachments.

8. **Family Relationships and Family Groups.** A document and all other documents in its attachment range, emails with attachments, and email, Electronic Communications,⁹ or other documents together with any documents referenced by document stubs or via links to internal document sources within those emails, Electronic Communications or other documents all constitute “Family Groups.”

9. If any member of a Family Group is produced, all members of that Family Group must be also be produced, except (1) any documents withheld or redacted on the basis of privilege or other applicable legally cognizable protection; and (2) any nonresponsive attachments that contain trade secrets; proprietary information; non-public commercial, financial, strategic, personnel, or regulatory information; other commercially sensitive material; or confidential material that may be subject to third-party notice provisions. If the Producing Party withholds or redacts a document under (1), the Producing Party shall comply with Section IV of Exhibit B to this Protective Order. If nonresponsive attachments are withheld under (2), the Producing Party must produce a placeholder TIFF image in place of each such document indicating that the document is nonresponsive.

10. All documents within a Family Group shall be produced together. Family Group relationships shall be preserved. Child files shall follow parent files in sequential Bates Number order, including in the case of Embedded Files¹⁰ produced separately from their parent.

⁹ “Electronic Communication” means a message transmitted electronically or digitally and includes emails, text messages, multi-media messages, communications from any social media platform (whether public or private posts or private messages) or messages from any chat application or chat feature (including Microsoft Teams, Slack, Skype, Zoom, Signal, Hangouts, Messenger, and WhatsApp), as well as any file (document, photo, video, audio, or otherwise) incorporated as an attachment or Embedded File or sent or received independently (that is, not accompanied by an electronic message containing text).

¹⁰ “Embedded File” means any document contained in or linked to another document, images embedded in documents, and documents referenced via links to internal document sources.

11. Scanning Hard-Copy Documents. In scanning hard-copy documents, each page should be output to a single page TIFF file.

12. Bates Numbers. Each page of a document produced in TIFF format and each electronic file produced in Native Format shall have a unique fixed-length numeric identifier (“Bates Number”) containing at least eight (8) digits. The Producing Party may choose its own alpha prefix but that prefix shall not change across productions. Child files shall follow parent files in sequential Bates Number order. Bates Numbers shall be electronically “burned” onto the image following the formatting requirements in Exhibit B. Unless it would obscure, conceal, or interfere with any information originally appearing in the underlying image, the Bates Number shall be burned on the lower right-hand corner of each image.

13. Metadata Fields and Processing. Each of the Metadata and coding fields set forth in Exhibit B that can reasonably and technically be extracted from a document shall be produced for that document. The Parties are not obligated to populate manually any of the fields in Exhibit B if such fields cannot be extracted from a document using reasonable means, with the exception of the following, if available: (a) BegBates, (b) EndBates, (c) BegAttach, (d) EndAttach, (e) Custodian, and (f) MD5 Hash or SHA-1 Hash. Metadata shall be provided in a modern load file format delimited file with a .DAT file extension and standard delimiters for column break and text qualifier. The first line shall be the header with field names, and each subsequent line shall contain the fielded data for each document. Nothing herein shall require a Producing Party to create or produce Metadata that does not exist or is not reasonably or technically accessible.

14. Production Media. The Producing Party shall produce Document images, Native Format files, Load Files, and Metadata on hard drives, CDs, DVDs, USB thumb drives, secure

FTP, or other mutually agreeable Media¹¹ (“Production Media”). Each piece of Production Media shall include a unique identifying label corresponding to the identity of the Producing Party, the date of the production of Documents on the Production Media, and the Bates Number ranges of the Documents in that production (e.g., “Defs.’ Production January 1, 2024, GORMAN_00000123-GORMAN_00000456”). To the extent that the Production Media includes any confidential information protected under the Protective Order, the label on such Production Media shall indicate that the Production Media includes information so designated as required under the terms of such order. Production Media shall also include text referencing the case name and number. Further, any replacement Production Media shall clearly identify that it is a replacement and cross-reference the Bates Number range that is being replaced. All Production Media that is capable of write protection should be write-protected before production. All Production Media shall be encrypted, with the Producing Party to provide a decryption key at the time of production. Productions should be accompanied by a cover letter identifying the Bates Numbers for Documents produced. All electronic transmissions of produced materials must be effected via a secure file transfer system.

15. Each Producing Party shall make reasonable efforts to process all ESI with the following time zone: Eastern / GMT-5.

I. Return of Confidential Material at Conclusion of Litigation

16. Within sixty (60) days of the conclusion of this litigation and any appeal thereof, all documents designated as Confidential or Highly Confidential under this Protective Order, including copies, duplicates, or extracts of such Discovery Material, or descriptions that disclose

¹¹ “Media” means an object or device, real or virtual, on which information or data is stored, including but not limited to digital or analog machine-readable devices, computers, Internet sites, portable storage media, servers, networks, cloud-based storage, discs, and tapes.

Confidential information from such Discovery Material, and not received in evidence (other than material subject to work product protection) shall be destroyed or returned to the Producing Party, at the option of the Receiving Party. Any work product that discloses information from Discovery Material designated Confidential or Highly Confidential under this Protective Order shall be destroyed. Counsel of record for each Party shall make written confirmations of compliance herewith and shall deliver the same to counsel for the Producing Parties not more than ninety (90) days after final termination of this litigation, along with executed copies of EXHIBIT A - ACKNOWLEDGEMENT AND DECLARATION OF COMPLIANCE obtained by such counsel. The Clerk of the Court may return to counsel for the Parties, or destroy, any sealed material at the end of the litigation, including any appeals.

J. Use of Discovery Material by the CFTC

17. Notwithstanding any of the foregoing terms, nothing in this Protective Order shall limit the CFTC's retention or use of any Discovery Material, including information designated by any Party to this Protective Order as Confidential or Highly Confidential, for any of the "Routine Uses of Information" identified in the applicable CFTC Privacy Act System of Records Notices, or as otherwise authorized, permitted, or required by statutes and regulations governing CFTC practice, policy and procedures, including without limitation, Sections 8 and 12 of the Commodity Exchange Act, the Federal Records Act and Freedom of Information Act.

K. Court Retains Jurisdiction

18. After the conclusion of this litigation, the provisions of this Protective Order shall continue to be binding and this Court shall retain jurisdiction over all persons who have access to Confidential or Highly Confidential Discovery Material produced pursuant to this Protective Order

for the purpose of enforcement of this Protective Order, including any appropriate sanctions for violations.

Dated: November 27, 2023

Respectfully submitted by:



Alyson Cohen
R. Stephen Painter, Jr.
Devin Cain
Benjamin Rankin
Commodity Futures Trading Commission
290 Broadway, 6th Floor
New York, NY 10005

Attorneys for the Plaintiff

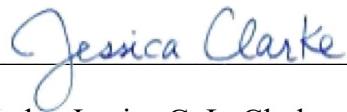


Sean Hecker
Michael Ferrara
Alysha M. Naik
Helen F. Andrews
KAPLAN HECKER & FINK LLP
350 Fifth Avenue, 63rd Floor
New York, New York 10118

Attorneys for the Defendant

Dated: December 4, 2023

SO ORDERED:



Judge Jessica G. L. Clarke
UNITED STATES DISTRICT JUDGE

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

COMMODITY FUTURES TRADING
COMMISSION,

Plaintiff,

v.

JOHN PATRICK GORMAN III,

Defendant.

Case No. 21-cv-870 (JGLC)

ECF Case

ACKNOWLEDGMENT AND DECLARATION OF COMPLIANCE

I hereby acknowledge that I have been given a copy of the Stipulated Protective Order dated _____, 2023, in the above-captioned case; that I have read the Stipulated Protective Order; and that I agree to be bound by it. I further understand and agree that I shall not disclose Confidential or Highly Confidential information or documents to others, except in accordance with the Stipulated Protective Order. I further understand and agree that my obligation to honor the confidentiality of such Confidential or Highly Confidential information or documents will continue even after the termination of this litigation. I further understand and agree that, in the event that I violate the terms of the Stipulated Protective Order, I will be subject to sanctions, including but not limited to sanctions by way of contempt of court. I further understand and agree to submit myself to the personal jurisdiction of this Court for matters pertaining to this acknowledgment and declaration.

(If executed within the United States, its territories, possessions or commonwealths) I declare under penalty of perjury that the foregoing is true and correct.

Executed on this _____ day of _____, _____ at _____ by

Signed: _____

(If executed outside of the United States) I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this _____ day of _____, _____ at _____ by

Signed: _____

EXHIBIT B
DOCUMENT PRODUCTION FORMATS

I. OVERVIEW

1. All Documents shall be produced: (1) as (i) Bates-stamped tagged image file format (“TIFF”) images, or (ii) where expressly required or permitted by this Exhibit, Native Format files compliant with the Native Format requirements detailed in Section IV of this Exhibit; and (2) along with (i) an image load/cross reference file, (ii) a data Load File with fielded Metadata, and (iii) document-level Extracted Text¹² for ESI or OCR¹³ Text for scanned hard-copy documents.

2. All produced documents shall comply with the applicable requirements set out in this Exhibit and in the Protective Order.

II. IMAGE REQUIREMENTS

3. Except as otherwise provided in this Protective Order, all documents shall be produced as TIFF images in 300 dpi Group IV single-page monochrome format.

4. All images shall be sequentially Bates-stamped, in accordance with the requirements set out in Section III of this Exhibit.

5. Images shall include the following content where present:

- a. For word processing files (e.g., Microsoft Word): Comments and “track changes” (and similar in-line editing).

¹² “Extracted Text” means text extracted from a Native Format file using standard e-discovery processing tools.

¹³ “Optical Character Recognition” or “OCR” means the process of recognizing and creating a file containing Searchable Text (the native text extracted or generated from a Document) within an image of a document. The latter text is also referred to as “OCR Text.” “Searchable Text” means the native text extracted or generated from a Document, including text generated from an electronic image of a Hard-Copy Document through OCR.

b. For presentation files (e.g., Microsoft PowerPoint): Speaker notes and comments.

6. Reasonable care shall be taken not to degrade the legibility of documents during the imaging process. If legibility is found to have been degraded, the Receiving Party may make reasonable requests for re-production of affected documents.

7. If particular documents warrant departure from these image requirements (e.g., production of color images instead of monochrome), the Parties shall cooperate to arrange for the mutually acceptable reasonable production of such Documents.

III. BATES STAMPING REQUIREMENTS

8. Each page of a document produced in image format shall have its Bates Number electronically “burned” onto the image, using a consistent length with leading zeros in the number, and consistent font and type size. The format of the Bates Numbers shall not change across productions.

9. Unless it would obscure, conceal, or interfere with any information originally appearing on the document, the Bates Number shall be burned on the lower right-hand corner of the document.

IV. NATIVE FORMAT REQUIREMENTS

10. Spreadsheet files

- a. Spreadsheet files (e.g., Microsoft Excel) shall be provided in Native Format.
- b. In lieu of a TIFF image version of each spreadsheet file, a Bates-stamped single-page TIFF placeholder file shall be produced along with the Native Format version of each file. The TIFF Placeholder should read “Document Produced Natively.”

- c. Spreadsheet files shall include the following content where present: hidden columns, rows, and sheets; comments; and “track changes” (and similar in-line editing).
- d. When redaction is necessary, a redacted TIFF image version shall be produced.

The Parties reserve the right to request access to the Native Format versions of such files.

11. Multi-media files

- a. Multi-media files (e.g., audio or video files) shall be provided in Native Format.
- b. In lieu of a TIFF image version of each multi-media file, a Bates-stamped single-page TIFF placeholder file shall be produced along with the Native Format version of each file. The TIFF Placeholder should read “Document Produced Natively.”
- c. If a Producing Party wishes to redact multi-media files for reasons other than to protect the privacy of individuals not party to this Action, the Parties shall meet and confer as to the bases for such redaction, the format of redaction to be applied, and the format of production for the unprotected portion of the content. The details of any such redaction would then need to be included in a privilege log in accordance with the protocols set out in Section E(9) of the Protective Order unless otherwise agreed to by the parties or ordered by the Court.

12. Other files

- a. In limited circumstances, it may be necessary to obtain or view the Native Format versions of files, including color documents/images and dynamic files, such as databases. The Parties reserve the right to request access to the Native

Format versions of such files and/or an image format that supports viewing color documents.

V. IMAGE LOAD/CROSS REFERENCE FILE REQUIREMENTS

13. A single-page image load/cross-reference file shall be provided with each production.

14. The file should use the Concordance Image Viewer (.OPT) format, as in the sample below. Note, the volume label information (“MSC001” in the sample .opt file) is optional:

Sample Concordance Image Viewer .opt file:

MSC000001, MSC001, MSC\0000\00000001.TIF, Y,,,3

MSC000002, MSC001, MSC\0000\00000002.TIF,,,

MSC000003, MSC001, MSC\0000\00000003.TIF,,,

MSC000004, MSC001, MSC\0000\00000004.TIF, Y,,,2

MSC000005, MSC001, MSC\0000\00000005.TIF,,,

VI. EXTRACTED TEXT/OCR TEXT REQUIREMENTS

15. Extracted Text and/or OCR Text shall be provided for all documents as separate, document-level text files; Extracted Text and/or OCR Text shall not be embedded in the .DAT file. Document-level text shall be produced.TXT format for each document, and filenames for .TXT files will be the Bates Number of the TIFF image of the first page of the corresponding document.

16. OCR Text shall be provided for all redacted documents in lieu of Extracted Text.

17. If a document is provided in Native Format with a single-page placeholder TIFF image (e.g., spreadsheet files), the text file shall contain the full Extracted Text of the native file.

18. With respect to produced text files, the specifications herein address ANSI text-based productions. Unicode text-based productions shall be provided for productions containing non-English language documents.

19. The Parties agree not to knowingly degrade the searchability of documents as part of the document production process. For example, Extracted Text should not be replaced by OCR Text except where appropriate (e.g., OCR for redacted documents).

VII. DATA LOAD FILE REQUIREMENTS

20. A data Load File shall be provided with each production.

21. The file shall be a Concordance-loadable data file (“.DAT” file) and contain Bates-stamp and Metadata information as detailed below.

22. The delimiters and qualifiers to be used in the .DAT file are:

- *Record delimiter:* Windows newline/Hard return (ASCII 010 followed by ASCII 13)
- *Field delimiter:* Pilcrow ¶ (ASCII 020)
- *Multi-value delimiter:* Semicolon (do not follow with space) ; (ASCII 059)
- *Text qualifier:* Small thorn þ (ASCII 254)
- *Substitute Carriage Return or New Line in data:* Registered Trademark ® (ASCII 174)

23. With respect to .DAT files, the specifications herein address ANSI text-based productions. Unicode text-based productions shall be provided for productions containing non-English language documents.

24. The .DAT file shall have a header line with the below listed field names and shall include the corresponding information per each applicable field:

Field	Comments	Document Types
Production:: Begin Bates	Beginning Bates Number.	All.
Production:: End Bates	Ending Bates Number.	All.
Production:: Begin Attach	Bates Number from the first page of each attachment.	Email only.
Production:: End Attach	Bates Number from the first page of each attachment.	Email only.
Production:: Image Count	Number of TIFF image pages in the produced Document.	All.
Number of Attachments	Number of attachments to an e-mail.	Email only.
File Extension	File extension of the original Document (e.g., .msg, .docx, .jpg).	All.
FileSize	File size of the original Document. Format: kilobytes.	All.
Unified Title	Subject of the document. If the document is an email, this field contains the email subject. If the document is not an email, this field contains the document's file name.	Non-Email files.
Custodian	Email: Mailbox in which the file was located. Other: Individual who originated the document. Format: LASTNAME, FIRSTNAME.	All.
All Custodian	For globally de-duplicated productions only. Full name of all Custodians for whom the Document is being produced. Format: LASTNAME, FIRSTNAME; LASTNAME, FIRSTNAME.	All.
Author	Author of Document from available Metadata.	Loose files and attachments.
Email From	Electronic Communication author.	Electronic Communications only.

Field	Comments	Document Types
Email To	Electronic Communication addressee(s)/recipients.	Electronic Communications only.
Email CC	Email addressee(s), carbon copy.	Email only.
Email BCC	Email addressee(s), blind carbon copy.	Email only.
Email Subject	Email subject.	Email only.
Created Date/Time	File creation date. Format: MM/DD/YYYY HH:MM AM/PM.	All.
Last Modified Date/Time	File modification date. Format: MM/DD/YYYY HH:MM AM/PM.	All.
Sent Date/Time	Electronic Communication sent date. Format: MM/DD/YYYY HH:MM AM/PM.	Electronic Communications only.
Sort Date/Time	Primary date field MM/DD/YYYY HHMM AM/PM. This is the parent date copied down to attachments.	All.
MeetingStartDate	Start date of calendar appointment. Format: MM/DD/YYYY	Calendar items only.
MeetingStartTime	Start time of calendar appointment. Format: HH:MM:SS AM/PM	Calendar items only.
MeetingEndDate	End date of calendar appointment. Format: MM/DD/YYYY	Calendar items only.
MeetingEndTime	End date of calendar appointment. Format: HH:MM:SS AM/PM	Calendar items only.
TimeZone	The time zone in which files were standardized during processing (e.g., ET / GMT-5).	All.
MessageID	Globally unique identifier for a message assigned by the host email system. This value is extracted from parent message during processing and typically includes messageid and a domain name (e.g.,	Email only.

Field	Comments	Document Types
	<0E6648D558F338179524D555@m1p.contoso.net).	
ConversationIndex	Email thread identification.	Email only.
Importance	Email flag indicating priority level set for message.	Email only.
Sensitivity	Sensitivity field from Email messages.	Email only.
Record Type	Descriptor for the type of document at the time of collection: “Email” for all e-mails; “Attachment” for files that were attachments to e-mails; “Audio” “Video” or “Photograph” for the applicable type of multi-media file; “Electronic Communication” for all files meeting the definition given in this Stipulation; “E-Document” for all other documents and files collected electronically; and “Hard-Copy Document” for Hard-Copy Documents that have been scanned and converted to an electronic image.	All.
FileName	Name of file as maintained in the ordinary course of business, at the time of collection.	Loose files and attachments.
Has Hidden Data	Denotes if file contains hidden content. Format: Yes/No value.	Loose files and attachments.
MD5 or SHA-1 hash	Unique file identifier.	All.
TextPath	The production deliverable path to the Extracted Text or OCR Text for the Document, including the file name.	All.
NativePath	The production deliverable path to the Native Format file for the Document, including the file name (if a Native Format file is provided).	Loose files and attachments.
ProdVol	Volume label information for the volume in which the document was produced.	All.

Field	Comments	Document Types
Confidential	Confidentiality level if assigned pursuant to the Protective Order. “Whole” for wholly confidential documents; “Part” for documents marked as partly confidential.	All.

25. In globally de-duplicated, incremental productions, there will be instances when production of documents from additional Custodians will include documents previously produced. A Custodian Append overlay Load File using the Load File format described above shall be provided with an updated AllCustodian field (BegBates and EndBates fields may be used as the unique identifiers). For globally and within custodian de-duplicated productions, a similar append overlay Load File shall be provided with an updated AllFilePaths field.